I.2 „Das perfekte Opfer“ – eine Analyse sicherheitsbezogener Einstellungen und Verhaltensweisen im Internet in Abhängigkeit der Nutzerpersönlichkeit

Henning Staar[1], Rafael Wilms[2], Judith Hinrichs[1]
[1] Fachhochschule für öffentliche Verwaltung NRW, Abteilung Duisburg
[2] Fachhochschule Südwestfalen, Fachbereich Ingenieur- und Wirtschaftswissenschaften

1 Einleitung

Insbesondere vor dem Hintergrund umfassender Digitalisierungsprozesse und der damit einhergehenden, stetig zunehmenden elektronischen Datenverarbeitung wird das Risiko des Diebstahls sensibler Informationen zu einem höchst relevanten Thema sowohl für Unternehmen als auch für Privatpersonen (Mitnick & Simon, 2006; Pohlmann & Linnemann, 2010). Eine zentrale Rolle in der Diskussion um Informations- und Datensicherheit spielt dabei „die einzige Schwachstelle im gesamten Sicherheitssystem [...], die man nicht ‚patchen' kann“ (Lipski, 2009, S. 7) – der Mensch (Baumann, Schimmer & Fendl, 2007; Schaumann, 2017). Diese Manipulation von Personen unter Ausnutzung gewisser Besonderheiten der menschlichen Psyche mit dem Ziel der Herausgabe diskreter Informationen wird in der Literatur als „Social Engineering“ oder auch als „Human Hacking“ bezeichnet (vgl. Bundesamt für Sicherheit in der Informationstechnik, 2003, 2011; Hadnagy, 2011, 2014). Sowohl im täglichen Leben als auch in Unternehmen kann Social Engineering zu immens hohen materiellen und immateriellen Schäden führen. Unternehmen haben dabei in erster Linie mit den enormen finanziellen Schäden zu kämpfen, die im Zuge eines erfolgreichen Social Engineering-Angriffs entstehen (Schumacher, 2013). Im Rahmen einer Spezialstudie zum Wirtschaftsschutz bat der deutsche Digitalverband Bitkom im Januar 2016 rund 350 der von Social Engineering-Angriffen betroffenen Industrieunternehmen, den für sie dadurch entstandenen finanziellen Schaden zu schätzen. Das Ergebnis verdeutlicht die gegenwärtige Relevanz des Themas aus betriebswirtschaftlicher Perspektive: Alleine in den letzten zwei Jahren kam es zu einer geschätzten Schadenssumme von 44,7 Milliarden Euro (Bitkom, 2016). Neben den erheblichen finanziellen Verlusten sind weitere typische Folgen von Social Engineering Angriffe auf Unternehmen Imageverlust, Verlust von Wettbewerbsvorteilen, Vertrauensverlust und Probleme mit Kunden oder Lieferanten infolge gestohlener personenbezogener Daten (ebd.). Eine bekannte Form des Social Engineerings stellt das sogenannte „Phishing“ dar (Long, Pinzon, Wiles & Mitnick, 2008): Hier werden Opfer beispielsweise über mehr oder weniger authentisch gefälschte E-Mails von vertrauenswürdigen Firmen, deren Dienste im Normalfall

freiwillig genutzt werden, auf präparierte Webseiten weitergeleitet, bei denen diese dann ihre privaten Zugangsdaten eingeben müssen (vgl. z.B. Lipski, 2009; Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010).

Jüngere theoretische Beiträge und empirische Studien zur Informations- und Datensicherheit widmen sich diesem Themenbereich des Social Engineering verstärkt interdisziplinär und rücken dabei neben täterbezogenen Analysen (z.B. Watson, Holz & Mueller, 2008) vor allem gruppen- bzw. kulturbezogenen Aspekte (Flores, Holm, Nohlberg & Ekstedt, 2014; Tembe et al., 2014) als auch individuelle Charakteristika wie Persönlichkeitsmerkmale der (potentiellen) Opfer in den Fokus (z.B. Uebelacker & Quiel, 2014; Pattinson, Jerram, Parsons, McCormac & Butavicius, 2012;Vishwanath, Herath, Chen, Wang & Raghav Rao, 2011). Trotz der gegenwärtigen intensiven Beschäftigung mit dem Thema fehlen jedoch weiterhin eindeutige bedingungs- und personenbezogene Handlungsimplikationen zum Umgang mit den genannten Formen des Datendiebstahls (Gupta, Tewari, Jain & Agrawal, 2017). Ein möglicher Grund mag in der vergleichsweise häufigen Reduktion individueller Charakteristika auf die zentralen Persönlichkeitsmerkmale („Big 5“; Rammstedt, Kemper, Klein, Beierlein & Kovalena, 2012) liegen. Zugrundeliegende Motive oder Werte von Personen werden hingegen bislang unzureichend betrachtet (Fazio, Blascovich & Driscoll, 1992). Darüber hinaus beziehen bislang nur wenige Studien sowohl umfassende psychologische Befragungsinventare zu sicherheitsbezogenen Einstellungen, Verhaltensweisen und individuellen Personenmerkmalen als auch die Beurteilung von E-Mails oder Websites hinsichtlich der Vertrauenswürdigkeit und Handlungsbereitschaft in ihre Analysen ein. Der vorliegende Beitrag verfolgt mit einem entsprechenden Studiendesign das Ziel, diese Lücke weiter zu schließen und Erkenntnisse zu personenbezogenen Einflüssen auf die Informations- und Datensicherheit zu generieren.

Der Beitrag gliedert sich wie folgt: Nach einer theoretischen Einführung in das Konstrukt Social Engineering sowie einer Darstellung des gegenwärtigen Forschungsstands zu dem Einfluss individueller Charakteristika auf die Anfälligkeit der Opferwerdung wird in Abschnitt 3 die Methode und das Studiendesign vorgestellt. Im Anschluss an die Darstellung der Ergebnisse in Abschnitt 4 schließt der Beitrag mit einer kritische Diskussion und Implikationen für Forschung und Praxis.

2 Social Engineering

Die theoretische Beschreibung und empirische Untersuchung von Social Engineering sowie deren Antezedenzien, Konsequenzen sowie potentiellen Einflussfaktoren ist weitreichend und komplex. Grundsätzlich bezeichnet Social Engineering in der IT-Sicherheit Angriffsmethoden, bei denen Personen durch bestimmte

Handlungen vom Angreifer manipuliert werden sollen. Ziel ist es, die Adressaten zu Handlungen zu bewegen, die für sie oder ihr Umfeld potentiell unvorteilhaft und schädigend sind, wie beispielsweise die Herausgabe sensibler und vertraulicher Informationen von Unternehmen oder Privatpersonen (Hadnagy, 2014; DATEV-Gesamtsicherheitsgremium & Deutschland sicher im Netz e.V., 2015). Dabei werden mittels psychologischer Techniken menschliche Eigenschaften und Schwächen ausgenutzt und bewusst soziale Beziehungen aufgebaut, um die Opfer anschließend effektiv auszunutzen (Fleischer, 2016; Lipski, 2009). Im Folgenden wird zunächst auf die unterschiedlichen Arten von Social Engineering sowie die Vorgehensweisen der Social Engineers eingegangen, um schließlich eine Einordnung des „Phishing"–Phänomens als einen der bekanntesten Social Engineering-Ansätze zu vertiefen.

2.1 Arten von Social Engineering

Social Engineering-Angriffe können auf unterschiedlicher Basis durchgeführt werden. Es werden daher allgemein drei Arten von Social Engineering unterschieden: Human-Based Social Engineering, Reverse Social Engineering und Computer-Based Social Engineering (Maro, 2012). Diese drei Formen werden im folgenden eingehender illustriert.

Beim Human-Based Social Engineering wird zum Großteil auf soziale Beziehungen gesetzt, Informationen werden durch eine direkte soziale Annäherung an die Person beschafft. Für diese Art des Angriffs benötigt der Social Engineer zum einen so viele Informationen wie möglich über die Person bzw. Organisation, die er angreift, zum anderen werden persuasive Einflusstechniken im direkten (virtuell vermittelten) Kontakt relevant (vgl. z.B. Staar, Keysers, Storch, Kempny & Janneck, 2015). Dafür stehen ihm diverse Möglichkeiten zur Verfügung, wie zum Beispiel die Kontaktaufnahme über das Telefon oder die Informationssammlung im Internet und in sozialen Netzwerken (Schumacher, 2013). Beim Reverse Social Engineering wird das Opfer dazu gebracht wird, seinem Angreifer freiwillig und aktiv die gewünschten Informationen zu übermitteln. Als kurzes Beispiel eignet sich folgendes Szenario: Der Angreifer schlüpft in die Rolle eines Supportmitarbeiters, stellt sich beim Opfer telefonisch als solcher vor und hinterlässt, vermeintlich netterweise, auch noch seine Telefonnummer für den Fall, dass ein Problem auftritt. Anschließend sorgt der Social Engineer mit seinen IT-Kenntnissen dafür, dass ein solches Problem tatsächlich auftritt und der Mitarbeiter den Support um Hilfe bittet. Nun ist es für den Angreifer ein Leichtes, von seinem Opfer eine Menge Informationen über Zugangsdaten und ähnlichem zu erfahren (Baumann, Schimmer & Fendl, 2007). Wie der Name bereits impliziert, erfolgt der Angriff beim Computer-Based Social Engineering durch technische Hilfsmittel und über den Computer. Dabei kommen Methoden wie Mailanhänge, Popup-Fenster oder manipulierte Internetseiten zum Einsatz.

(Baumann, Schimmer & Fendl, 2007). Wie im folgenden Abschnitt noch detaillierter dargestellt wird, nutzen Social Engineers im Rahmen des Computer-Based Social Engineering zudem oft Phishing und Vishing, um Informationen zu sammeln.

Hadnagy (2014) kommt mit Blick auf die unterschiedlichen Arten des Social Engineering zu dem Schluss *„keine Information ist nutzlos"* (S. 56). Folglich geht es vorwiegend darum, die Abläufe in Unternehmen zu durchschauen und auf Charakteristika der Zielpersonen, deren Stärken und Schwächen, sowie ihren sozialen Interaktionen im Alltag und ihre Art, zu kommunizieren. Für das Sammeln von Informationen im Rahmen des Social Engineerings haben sich im Laufe der Jahre viele Quellen und Methoden entwickelt. So reichen die Wege von kontaktfreien Ansätzen wie *„Trashing"* oder „Dumpster Diving" (Long et al., 2012), welche das Absuchen von Abfallcontainern von Firmen und Unternehmen nach interessanten und hilfreichen Informationen beschreiben, über telefonischen (Stöcker, 2011) oder Face-to-Face-Kontakt (Baumann, Schimmer & Fendl, 2007) bis hin zu *„Lauschangriffen"* über das Internet (ebd.). Bei letzterem geht es auch um das generelle Sammeln von Informationen und Daten, mit der Besonderheit, dass das Opfer dabei nicht bewusst, sondern indirekt vermittelt mit dem Social Engineer in Kontakt tritt. Daher fallen unter den Begriff „Lauschangriff" auch die indirekten und unpersönlichen Angriffe, bei denen das Internet zu Hilfe genommen wird. Oft begegnen einem hierbei Begriffe wie Malware, Spyware, Phishing oder Vishing. Diese werden im folgenden Abschnitt näher erläutert.

2.2 Internet-basierte Methoden der Informationssammlung

Die Verbreitung von sogenannter „Malware" äußert sich durch die unbemerkte Installation von verschiedenen Programmen auf dem Rechner des Opfers, die bei diesen Schäden verursachen, da sie in der Lage sind, zum Beispiel Tastatureingaben mitzulesen oder sogar den Computer fernzusteuern und das Opfer somit effektiv auszuspionieren (DATEV-Gesamtsicherheitsgremium & Deutschland sicher im Netz e.V., 2015). Laut einer Studie der Firma „Panda Security", ist durchschnittlich jeder vierte Computer in Deutschland mit einer Malware infiziert (Röttgerkamp, 2018). Als Beispiele für solche Schadprogramme, die vielen zumindest vom Namen her geläufig sind, lassen sich Viren oder Trojaner nennen. Diese werden über die Anhänge von E-Mails oder über manipulierte Internetseiten verbreitet (DATEV-Gesamtsicherheitsgremium & Deutschland sicher im Netz e.V., 2015). Auch das sogenannte „Phishing" ist mittlerweile Gegenstand sowohl wissenschaftlicher Studien als auch praktischer Empfehlungen im Umgang mit Datensicherheit im Internet. Dessen ungeachtet wird eine Vielzahl von Nutzern noch immer Opfer von gefälschten E-Mails oder Websites, die nach Passwörtern oder Bankdaten fragen. Phishing leitet sich von dem englischen Wort für „Fishing" ab, was so viel wie Angeln bedeutet.

Über authentisch gefälschte E-Mails, von vertrauenswürdigen Firmen, wie PayPal oder Ebay, deren Dienste im Normalfall freiwillig genutzt werden, leiten Social Engineers ihre Opfer auf präparierte Webseiten weiter, bei denen diese dann ihre privaten Zugangsdaten eingeben müssen. Die Angreifer begründen diese Anfragen beispielsweise mit der Verbesserung der Kontosicherheit oder einem ähnlichen Vorwand, der dem Kunden am Herzen liegt. Sie *„angeln"* also nach den persönlichen Daten ihrer Opfer (DATEV-Gesamtsicherheitsgremium & Deutschland sicher im Netz e.V., 2015). Eine Abwandlung des Phishings stellt das „Vishing" dar. Abgeleitet ist dieser Begriff von der Langform *„Voice Fishing"*. Hierbei nutzen Angreifer die geringen Kosten der Internettelefonie, um mittels eines Ansagetextes in kurzer Zeit eine große Anzahl Telefongespräche zu führen. Hierbei wird beispielsweise behauptet, dass eine Kreditkarte verloren gegangen sei. Um eine Sperrung oder Ähnliches zu veranlassen, sollen dann PIN- oder TAN-Codes über die Telefontastatur eingegeben werden. So können die Social Engineers schnell und einfach sensible Daten abfragen (Dunham, 2008). Insofern als Phishing eine der verbreitetsten Computer-Based Social Engineering-Methoden und größten Gefahren vor allem für Unternehmen darstellt (Sans, 2017), wird in der im Rahmen des vorliegenden Beitrags durchgeführten Studie auf dieses Phänomen der Fokus gelegt.

2.3 Anfälligkeit für Social Engineering in Abhängigkeit von der Nutzerpersönlichkeit

In einem theoretischen Beitrag fassen Uebelacker und Quiel (2014) die Persönlichkeitsmerkmale Extraversion, Neurotizismus, Offenheit für Neues, Gewissenhaftigkeit und Verträglichkeit in ihrer Interaktion mit Anfälligkeit für Social Engineering-Angriffe zusammen. Während für Gewissenhaftigkeit, Extraversion und Offenheit beide Wirkrichtungen als möglich eingestuft werden, gehen die Autoren bei hohen Verträglichkeitswerten auch von einer hohen Anfälligkeit aus, das Gegenteil nehmen sie bei hohen Neurotizismus-Werten an. Cho et al. (2016) kommen in ihrer Studie hingegen zu dem Ergebnis, dass Verträglichkeit und Neurotizismus den größten Einfluss auf die wahrgenommene Vertrauenswürdigkeit von E-Mails und Webseiten habe, vor allem bei niedriger Ausprägung von Offenheit und Gewissenhaftigkeit (Cho, Cam & Oltramari, 2016). Butavicius und Kollegen (2017) identifizieren hingegen vornehmlich bei Personen mit hohen Verträglichkeitswerten als auch bei solchen, die psychisch stabil (im Sinne niedriger Neurotizismus-Werte) sind, eine hohe Fähigkeit, gefälschte Webseiten zu erkennen. Andere Forscher in diesem Bereich tragen diesen heterogenen Ergebnissen Rechnung und weisen darauf hin, dass möglicherweise andere gruppen- oder personenbezogenen Faktoren in die Analysen einzubeziehen sind, um aussagekräftigere Ergebnisse zu erhalten (z.B. Vishwanath et al., 2011). Werte- bzw. Motivstrukturen im Sinne individueller Einstellungs- und Verhaltensmuster sind in der psychologischen Forschung umfassend

betrachtet worden (Steinmetz, Schmidt, Tina-Booh, Wieczorek & Schwartz, 2009). Im Themenbereich um Social Engineering hingegen werden diese Faktoren bislang unzureichend in die Überlegungen einbezogen. Die Forschergruppe um Parsons (2017) hat mit der Entwicklung und Validierung ihres Human Aspects of Information Security Questionnaire (HAIS-Q) einen wesentlichen Beitrag geleistet, indem sie anhand ihres 63 Items-umfassenden Inventars sowohl Wissen um, Einstellung zu und Verhalten in Bezug auf eine Reihe sicherheitsrelevanter Foki legen. Gleichzeitig steht eine Betrachtung möglicher Konvergenzen zwischen sicherheitsbezogenen Einstellungen und Verhaltensweisen einerseits und Persönlichkeitsmerkmalen und individuellen Werten andererseits bislang noch aus.

In diesem Sinne sollte in der vorliegenden Studie (1) das konkrete Einschätzen von möglichen Phishing-Webseiten im Hinblick auf die Vertrauenswürdigkeit und Handlungsbereitschaft, den Anweisungen Folge zu leisten, in Beziehung gesetzt werden zu den Persönlichkeitsmerkmalen und den Wertetypen. Darüber hinaus sollten (2) diese beiden personenbezogenen Faktoren und allgemeinen sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet auf mögliche Zusammenhänge geprüft werden. Da sich, wie oben beschrieben, die bisherige Forschungslage noch uneindeutig zeigt, wurde von konkreten Hypothesen abgesehen und ein explorativer Ansatz gewählt.

3 Methode

Im Folgenden werden das Studiendesign, die Stichprobenakquise sowie die in der Befragung verwendeten Messinstrumente eingehender beschrieben.

3.1 Design und Messinstrumente

Die Studie wurde von Juni bis Juli 2018 an verschiedenen Fachhochschulen in NRW durchgeführt und richtete sich an Studierende unterschiedlicher Studiengänge. Der link zur Online-Befragung wurde über Kursverteiler sowie intern durch Studierende verteilt. Die Teilnahme war freiwillig.

Um die formulierten Fragestellung beantworten zu können, wurde neben der Erhebung soziodemographischer Daten sowie Fragen zum Internetverhalten eine Skala zu sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet, ein Fragebogen zur Persönlichkeitsmessung und zu den Werte-Typen verwendet. Weiterhin wurde eine Kurzskala zur Risikobereitschaft im Allgemeinen angewandt. Schließlich wurden verschiedene Seiten präsentiert, die die Teilnehmer hinsichtlich der Vertrauenswürdigkeit und der Handlungsbereitschaft, den Anweisungen Folge zu leisten, einschätzen sollten.

In Bezug auf die soziodemographischen Fragen wurden Alter, Geschlecht, Studienrichtung und der zukünftige Abschluss erhoben. In Bezug auf das Internetverhalten wurde nach Präferenzen, Nutzungshäufigkeit sowie nach der Nutzung verschiedener Dienste gefragt. Weiterhin wurde Medienkompetenz mittels drei Items erfragt, die aus einer früheren Studie stammen (Autoren, Jahr). Das Werte-Konzept dient dem Verständnis von individuellen Einstellungs- und Verhaltensmustern sowie dem Funktionieren von Organisationen, Institutionen und Gesellschaften (Hofstede, 1980; Schein, 1985). Für die vorliegende Studie wurden Skalen einer deutschen validierten Version des Portraits Value Questionnaire verwendet (Steinmetz, Schmidt, Tina-Booh, Wieczorek & Schwartz, 2009), welche ursprünglich zehn motivational unterschiedliche Wertetypen fasst. Für die Befragung wurden lediglich die fünf Wertetypen Macht, Leistung, Hedonismus, Stimulation und Selbstbestimmung auf einer sechsstufigen Skala erfasst. Zur Erfassung der Persönlichkeitsausprägung wurde das 10-Item Big Five Inventory (BFI-10) herangezogen. Dieses umfasst die fünf Persönlichkeitsdimensionen („Big 5“) Extraversion, Verträglichkeit, Gewissenhaftigkeit Neurotizismus und Offenheit für Erfahrung. Die Items wurden über eine fünfstufige Ratingskala (1 = „trifft überhaupt nicht zu“ bis 5 = „trifft voll und ganz zu“) beantwortet (Rammstedt, Kemper, Klein, Beierlein & Kovalena, 2012). Die Kurzskala R- misst die selbsteingeschätzte Risikobereitschaft einer Person mittels eines Items mit dem folgenden Wortlaut: „Wie schätzen Sie sich persönlich ein: Wie risikobereit sind Sie im Allgemeinen?“ Die Befragten geben ihre Einschätzung auf einer siebenstufigen Antwortskala von 1 = „gar nicht risikobereit“ bis 7 = „sehr risikobereit“ an. Der R-1 soll überprüfen, ob es Unterschiede zwischen den Studierenden hinsichtlich der Risikobereitschaft im Allgemeinen gibt. Um verschiedene Aspekte sicherheitsbezogener Einstellungen und Verhaltensweisen im Internet abbilden zu können, wurde auf ein selbst entwickeltes Inventar zurückgegriffen, das mit insgesamt 16 Items ein Screening ermöglichen soll, und weniger bereichsspezifisch als der HAIS-Q sicherheitsrelevante Aspekte erfragt (Autoren, Jahr). Die auf einer 5-Punkt-Likert Skala (1 = „trifft gar nicht zu“ bis 5 = „trifft völlig zu“) einzuschätzenden Subskalen zielen auf das wahrgenommen Risikopotenzial im Internet (6 Items; z.B. „Im Internet gibt es viele Möglichkeiten, Opfer von Betrug oder schädlichen Programmen zu werden“), die Selbstwirksamkeitserwartung (3 Items, z.B. „Gegen Internetangriffe kann man sich im Grunde fast nicht schützen“), das vorbereitende Sicherheitsverhalten (3 Items; z.B. „Meine Anti-Viren-Software ist immer auf dem aktuellen Stand“) sowie das In-Situ Sicherheitsverhalten (3 Items, z.B. „Persönliche Daten gebe ich nur nach sorgfältiger Prüfung der Seriosität einer Internetseite ein“). Zusätzlich wurde durch ein Einzelitem erfragt, ob die Person bereits Opfer von schädlichen Programmen oder Betrug im Internet geworden sei.

Die durch die Teilnehmer einzuschätzenden E-Mails wurden, um Konfundierungen zu vermeiden, alle aus öffentlichen Screenshots des Bezahldienstes Paypal ausgewählt. Insgesamt wurden nacheinander vier verschiedene Seiten präsentiert, welche die Teilnehmer hinsichtlich der Vertrauenswürdigkeit und der Handlungsbereitschaft, den Anweisungen Folge zu leisten, auf einer fünfstufigen Skala (1 = „stimme gar nicht zu“ bis 5 = „stimme voll zu“) einschätzen sollten. Um verschiedenartige Inhalte möglicher Phishing-E-Mails darzustellen, wurden folgende Situationen verwendet. Situation 1 bezieht sich auf eine Umstellung auf das SEPA-Verfahren, Situation 2 weist auf die Möglichkeit eines Zahlungsausfalls hin, in Situation 3 wurde der Hinweis auf kostenlose Retouren gegeben, Situation 4 bat um Verifizierung für ein Sicherheitsupdate. Alle E-Mail-Situationen wiesen links auf, bei allen war zudem der gleiche Absender (“Paypal“) ausgewiesen. Bis auf Situation 3 handelte es sich um Phishing-Versuche, die offizielle E-Mail von Paypal sollte als Kontrollsituation dienen.

4 Ergebnisse

Insgesamt nahmen $N = 77$ Studierende an der Befragung teil. 64 Prozent waren weiblich, der überwiegende Anteil der Teilnehmer gab ein Alter zwischen 21 und 25 Jahren an. Knapp 38 Prozent ordneten sich den Rechts- oder Wirtschaftswissenschaften zu, 17 Prozent dem Bereich „Medien und Kommunikation“, 11 Prozent entfielen auf Gesellschafts- und Sozialwissenschaften.

Die Ergebnisse dieser Studie wurden mittels des Statistikprogramm R Cran (2018) berechnet. Da es sich um eine explorative Studie handelt, wurden die Pearson-Korrelationskoeffizienten sowie deren Signifikanzniveau erzeugt. Der Ergebnisteil dieser Studie ist in zwei Abschnitte unterteilt. Der erste Abschnitt stellt den Einfluss der Big Five und der Wertetypen auf die Tendenz einer Phishing-Email zu vertrauen sowie den Anweisungen dieser zu folgen dar (Siehe Tabellen 1-2). Im zweiten Abschnitt der Ergebnisse wird das Inventar zu sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet mittels der oben beschriebenen Subskalen mit den unterschiedlichen Persönlichkeitsmerkmalen und Werten in Zusammenhang gebracht.

4.1 Beurteilung von E-Mails, Persönlichkeit und Werte des Nutzers

Tabelle 1 illustriert, dass sich hinsichtlich des Geschlechts keine Zusammenhänge zu Ausprägungen in den Persönlichkeitsmerkmale feststellen lassen. Mit Blick auf die Evaluationen der E-Mails spielt es zudem offenbar keine Rolle, ob der Teilnehmer selbst Paypal als Dienst nutzt. Interessanterweise korreliert die Selbsteinschätzung der Medienkompetenz positiv mit der Handlungsbereitschaft auf eine der Phishing-E-Mails (S2). Die Zusammenhänge in der Tabelle verdeutlichen weiterhin, dass die Phishing-Emails einmal weniger (S2), einmal ungefähr gleich (S4) und einmal als

deutlich vertrauenswürdiger eingeschätzt wurden (S1). Interessanterweise befindet sich die offizielle Paypal-Email (S3) in der Beurteilung im Mittelfeld. User können offenbar auch offizielle E-Mails nur unzureichend richtig beurteilen. Bei den Big Five zeigt sich, dass Neurotizismus positiv mit der Bereitschaft korreliert, den Anweisungen der zweiten Phishing-Email (Möglichkeit eines Zahlungsausfalls) Folge zu leisten. Dieses Ergebnis widerspricht den Überlegungen von Uebelacker und Quiel (2014), deckt sich aber mit denen von Cho et al. (2016). Bei den Wertetypen (siehe Tabelle 2) zeigt sich zum einen, dass der Wertetyp Macht positiv mit der Einschätzung der Vertrauenswürdigkeit der ersten Phishing-Email korreliert. Hohe Ausprägungen in den Werten Hedonismus und Stimulation zeigen sowohl im Phishing- als auch im offiziellen E-Mail-Beispiel signifikante positive Zusammenhänge zur Einschätzung der Vertrauenswürdigkeit und Handlungsbereitschaft. Menschen, denen vornehmlich der Spaß wichtig ist und solche, die Abenteuer eingehen erweisen sich also als vergleichsweise weniger argwöhnisch und weniger zögerlich, den links der E-Mails zu folgen. Interessant ist darüber hinaus das Ergebnis, dass das Geschlecht einerseits und sowohl die Einschätzung der Vertrauenswürdigkeit als auch die Bereitschaft, Folge zu leisten, signifikante Zusammenhänge aufweisen: Weibliche Teilnehmer erwiesen sich als vertrauens- und handlungsbereiter.

4.2 Sicherheitsbezogene Einstellungen, Verhaltensweisen, Persönlichkeit und Werte des Nutzers

Zusätzlich zu der Evaluation der vier E-Mail-Beispiele wurden die Teilnehmer mittels eines Inventars zu sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet befragt. Die Ergebnisse dieser Selbsteinschätzungen wurden ebenfalls in Zusammenhang zu Persönlichkeitsmerkmalen und Werten gebracht. Erwartungsgemäß korreliert die Selbstwirksamkeitserwartung mit beiden Aspekten des Sicherheitsverhaltens positiv auf dem .01-Niveau. Medienkompetenz korreliert positiv mit dem wahrgenommenen Risiko im Internet. Entgegen der obigen Ergebnisse zu Neurotizismus zeigen sich nur in der Tendenz negative Zusammenhänge ($r = .18$) zum In Situ-Sicherheitsverhalten, jedoch signifikante negative Korrelationen zur Risikobereitschaft ($r = .32^{**}$). Das bedeutet, das psychisch instabilere Menschen in der Tendenz weniger genau Webseiten oder E-Mails prüfen, bevor sie Daten eingeben. Möglicherweise kommen Menschen mit hohen Ausprägungen auf dieser Persönlichkeitsdimension gar nicht erst in Situationen, in denen ein sicherheitsrelevantes Reagieren notwendig wird bzw. können einen durch eine Phishing-E-Mail aufgebaute Dissonanz- bzw. Unsicherheitszustand weniger gut ertragen. Selbstbestimmung hingegen korreliert positiv sowohl mit dem vorbereitenden ($r = .32^{**}$) als auch mit dem In Situ-Sicherheitsverhalten ($r = .27^{*}$). Die Erfahrungen mit Betrug oder Schadsoftware zeigte keine Zusammenhänge zu sicherheitsbezogenen Einstellungen und Verhaltensweisen. Äquivalent zu den oben

dargestellten Ergebnissen zeigt sich auch hier ein signifikanter Zusammenhang des Geschlechts zum vorbereitenden (r = -.28*) als auch zum In Situ-Sicherheitsverhalten (r = .48**). Interessanterweise scheinen Erfahrungen mit Schadsoftware oder Online-Betrug keine Auswirkungen auf die sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet zu haben. Die Ergebnisse werden in der nachfolgenden Diskussion eingehend erörtert.

Tabelle 1: Mittelwerte, Standardabweichungen und Korrelationen

Variable	M	SD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Extraversion	3.62	1.02															
2. Verträglichkeit	2.91	0.76	-.10														
3. Gewissenhaftigkeit	3.56	0.79	.22	-.12													
4. Neurotizismus	2.79	0.86	-.36**	-.06	-.34**												
5. Offenheit	3.44	1.08	.06	-.03	.07	.01											
6. Medienkompetenz	4.01	0.63	.00	-.02	-.06	-.35**	.22										
7. Geschlecht	1.56	0.50	.10	-.12	-.11	.21	-.11	-.18									
8. PayPal	0.65	0.48	-.07	.02	-.13	-.14	.09	.10	-.05								
9. S1_ Vertrauen	3.29	1.28	.12	.03	-.07	-.18	-.15	.21	.06	.08							
10. S1_ Anweisung	3.05	1.41	.04	-.09	-.01	-.03	-.12	.06	.22	.10	.79**						
11. S2_ Vertrauen	1.95	1.12	-.16	.03	-.01	.16	-.03	-.20	.33**	-.13	.20	.27*					
12. S2_ Anweisung	1.94	1.25	-.13	-.04	-.00	.23*	.02	-.09	.37**	-.17	.19	.34**	.89**				
13. S3_ Vertrauen	2.86	1.30	.04	.05	-.10	.04	.12	.18	-.08	.11	.25*	.26*	.00	.05			
14. S3_ Anweisung	2.65	1.35	.08	.03	-.13	.06	-.04	.09	-.10	.01	.24*	.26*	.02	.10	.85**		
15. S4_ Vertrauen	2.66	1.24	.12	-.04	.06	-.02	-.00	.07	.20	-.07	.35**	.38**	.30**	.38**	.11	.15	
16. S4_ Anweisung	2.55	1.29	.03	-.10	.02	.11	-.03	-.05	.28*	-.20	.30**	.45**	.37**	.45**	.19	.31**	.85**

Anmerkung. M und *SD* werden genutzt, um den Mittelwert und die Standardabweichung zu repräsentieren. S1 steht für die erste Situation, in der eine Person einer Phishing-Email ausgesetzt wird, wobei die Nummern auf das Szenario verweisen. * bezeichnet $p < .05$. ** bezeichnet $p < .01$.

Tabelle 2: Mittelwerte, Standardabweichungen und Korrelationen

Variable	M	SD	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Macht	3.46	1.03													
2. Leistung	3.96	1.04	.68**												
3. Hedonismus	4.55	0.79	.28*	.31**											
4. Stimulation	3.64	0.97	.51**	.43**	.51**										
5. Selbstbe-stimmung	4.56	0.66	.31**	.29*	.29**	.53**									
6. Risikobereit-schaft	4.12	1.36	.47**	.41**	.36**	.72**	.37**								
7. S1_ Vertrauen	3.29	1.28	.26*	.18	.09	.21	-.13	.22							
8. S1_ Anweisung	3.05	1.41	.19	.10	.05	.15	-.12	.14	.79**						
9. S2_ Vertrauen	1.95	1.12	-.06	.01	-.07	-.13	-.14	-.07	.20	.27*					
10. S2_ Anweisung	1.94	1.25	-.02	.01	-.04	-.04	-.08	-.06	.19	.34**	.89**				
11. S3_ Vertrauen	2.86	1.30	.18	.16	.10	.14	.07	.21	.25*	.26*	.00	.05			
12. S3_ Anweisung	2.65	1.35	.14	.14	.17	.15	-.04	.17	.24*	.26*	.02	.10	.85**		
13. S4_ Vertrauen	2.66	1.24	.05	.16	.27*	.35**	.18	.23*	.35**	.38**	.30**	.38**	.11	.15	
14. S4_ Anweisung	2.55	1.29	-.02	.07	.26*	.27*	.10	.20	.30**	.45**	.37**	.45**	.19	.31**	.85**

Anmerkung. M und *SD* werden genutzt, um den Mittelwert und die Standardabweichung zu repräsentieren. S1 steht für die erste Situation, in der eine Person einer Phishing-Email ausgesetzt wird, wobei die Nummern auf das Szenario verweisen. * bezeichnet $p < .05$. ** bezeichnet $p < .01$.

5 Diskussion und Ausblick

Zusammenfassend zeigen die Ergebnisse, dass weder die untersuchten Big 5 noch die Wertetypen in Gänze Aussagekraft zu sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet haben. Neurotizismus zeigt sich, obgleich in divergierender Form, als aussagekräftigste Eigenschaft. Hinsichtlich der Werte

sind Stimulation und Hedonismus zentrale Treiber für die Einschätzung von Vertrauenswürdigkeit von E-Mails und der Bereitschaft, den Anweisungen Folge zu leisten. User, die in ihrem Online-Verhalten verstärkt nach Vergnügen und Genuss streben, sind den Ergebnissen zufolge also leichtere Opfer. Interessanter ist möglicherweise die Beurteilung der offiziellen E-Mail von Paypal zu bewerten. Es zeigte sich, dass User diese nicht trennscharf von den Phishing-Beispielen abgrenzen konnten. Folglich kann es nicht nur darum gehen, Personen auf mögliche Phishing-Hinweise aufmerksam zu machen, sondern Möglichkeiten zu etablieren, Sicherheit zu garantieren. Gleichwohl weisen Autoren wie Lipski (2009) darauf hin, dass es ein „Wasserzeichen" in diesem Kontext eben nicht gebe. Daneben ist vor allem der Faktor Geschlecht auffällig: Die weiblichen Teilnehmer der vorliegenden Studie zeigten sowohl in der Beurteilung des Inventars zu sicherheitsbezogenen Einstellungen und Verhaltensweisen im Internet als auch in der Evaluation der E-Mails weniger Bedenken. Welche geschlechtsspezifischen Charakteristika, die unabhängig von Persönlichkeit, Werten oder Medienkompetenzen sind, hier ursächlich sind, bedarf in jedem Falle weiterer Forschung. Möglicherweise können Einflussfaktoren wie der „Glaube an eine gerechte Welt" (Montada & Lerner, 1998) oder geschlechtsspezifische Besonderheiten digitaler Kommunikation im Hinblick auf z.B. Kooperation (vgl. z.B. Janneck, 2007) an dieser Stelle wichtige Erkenntnisträger sein. Weiterhin ist das Ergebnis bemerkenswert, dass bereits gemachte Opfererfahrungen mit Online-Betrug keinen Einfluss auf Sicherheitseinstellungen und –handeln hatten. Eine Sensibilisierung gerade dieser Gruppe wäre zu erwarten gewesen. Möglicherweise sind aber gerade stabile Wahrnehmungs- und Beurteilungsmuster ursächlich dafür, dass diese Personen Opfer werden konnten und möglicherweise erneut zu einem werden.

Im Folgenden wird noch auf methodische Schwächen sowie Grenzen der Arbeit näher eingegangen, Implikationen werden abgeleitet und ein Ausblick gegeben. An der Befragung haben 77 Personen vollständig teilgenommen. Zur Bestätigung signifikanter Zusammenhänge wäre eine Stichprobe größeren Umfangs nötig gewesen. Die Akquise von Personen, die sich einem solchen komplexen Design, welches mit erheblichem Zeitaufwand für die Teilnehmer verbunden ist, widmen, stellt hierbei die Schwierigkeit dar. Des Weiteren ist anzumerken, dass die Auswahl der Skalen für die vorliegende Befragung kritisch zu reflektieren ist. So wurde im Persönlichkeitsfragebogen mit jeweils zwei Items ein Konstrukt gemessen. Für eine tiefgreifende Untersuchung der Persönlichkeit wäre die deutsche Fassung des NEO-Persönlichkeitsinventars nach Costa und McCrae von Ostendorf und Angleitner (2004) heranzuziehen. Dieses Inventar umfasst die Persönlichkeit mit 240 Items, sodass eine differenzierte Messung der Hauptskalen durch 30 Facetten möglich ist (Happy, 2016).

Weiterhin wurden die Situationen im Fragebogenverlauf nicht in randomisierter Reihenfolge dargeboten. Folglich ist nicht auszuschließen, dass Teilnehmer nach der Darbietung der ersten Situation in ihren weiteren Einschätzungen bereits sensibilisiert waren, was zu einer Verzerrung der Antworten geführt haben könnte.

Bei einem solch sensiblen Thema besteht außerdem grundsätzlich die Möglichkeit, dass die Befragten im Sinne der „sozialen Erwünschtheit" geantwortet haben. Aufgrund der wiederholten Medienberichte über Datenmissbräuche und -diebstahl stellt sich zudem vermehrt eine Skepsis gegenüber solch präsentierten Inhalten ein.

Abseits der dargestellten Beschränkungen lassen die Ergebnisse praktische Implikationen durchaus zu. Beispielsweise könnte (auf Basis der Persönlichkeits- und Wertestruktur) die Ermittlung von „Risikoprofilen" in der Selbsteinschätzung hinsichtlich der Anfälligkeit, Opfer von Online-Betrug oder Schadsoftware zu werden, Personen sensibilisieren. Gepaart mit konkretem Handlungswissen wird eine gefahrenfreie Nutzung des Internets wahrscheinlicher. Auch das Arbeiten mit E-Mail-Beispielen kann zum einen die Identifikation eindeutiger Phishing-E-Mails fördern, zum anderen – so legen zumindest die Ergebnisse der Studie nahe – werden User ihrer Kontrollillusion beraubt, „richtig" von „falsch" immer unterscheiden zu können. Unternehmen hingegen müssen verstehen, dass sowohl Gestaltung, Inhalt sowie Häufigkeit von E-Mails an die Kunden Einfluss auf die Beurteilung der Vertrauenswürdigkeit und Handlungsbereitschaft haben werden. Zumindest in der vorliegenden Studie war dieser Rauschabstand der offiziellen E-Mails zu Phishing-E-Mails nicht gegeben. Zukünftige Studien sollten diese Erkenntnisse aufgreifen und Möglichkeiten und Grenzen herausarbeiten, wie Vertrauen durch Unternehmen trotz dieser Herausforderungen virtuell zu reproduzieren ist, und gleichzeitig eigenverantwortliches, sicherheitsbewusstes Verhalten auf Seiten des Users gestärkt werden kann. Insbesondere letzteres scheint ein wesentlicher Ansatzpunkt, um dem mittlerweile selbstverständlich vernetzten Alltag nicht nur erfolgreich und gefahrenfrei begegnen, sondern auch die vielfältigen Vorteile der Teilhabe am Netzgeschehen umfassend nutzen zu können.

6 Literatur

Baumann, U., Schimmer, K. & Fendl, A (2007). Faktor Mensch. Die Kunst des Hackens oder warum Firewalls nichts nützen. SAP Pocketseminar. SAP AG.

Beierlein, C., Kovaleva, A., Kemper, C. J. & Rammstedt, B. (2015). Kurzskala zur Erfassung der Risikobereitschaft (R-1). Zusammenstellung sozialwissenschaftlicher Items und Skalen. Verfügbar unter: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-426708 [12.07.2018]

Bitkom (2016). Spezialstudie Wirtschaftsschutz. Berlin: Bitkom Research GmbH .

Bundesamt für Sicherheit in der Informationstechnik (2011). IT-Grundschutz. Social Engineering. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042 [02.05.2018]

Bundesamt für Sicherheit in der Informationstechnik (2003). Studie. Durchführungskonzept für Penetrationstests. Bonn: BSI.

Butavicius, M., Parsons, K., Pattinson, M. & McCormac, A. (2015). Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails. In F. Burstein et al (Eds.) Proceedings of Australian Conference of Information Systems.

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. & Lillie, M. (2017). Understanding Susceptibility to Phishing Emails: Assessing the Impact of Individual Differences and Culture. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017).

Costa, P. T. & McCrae, R. R. (1995). Domains and Facets: Hierarchical Personality Assessment Using the Revised NEO Personality Inventory. Jounal of Personality Assessment, 64(1), 21–50.

Cho, J., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 7–13.

DATEV-Gesamtsicherheitsgremium & Deutschland sicher im Netz e.V. (2015). Verhaltensregeln zum Thema „Social Engineering“. Spezialausgabe: Leitfaden für Mitarbeiter. Berlin: Deutschland sicher im Netz e.V.

Dunham, K. (2008). Mobile Malware Attacks and Defense. Burlington: Syngress.

Fazio, R. H., Blascovich, J. & Driscoll, D. (1992). On the functional value of attitudes. Personality and Social Psychology Bulletin, 18, 388–401.

Fleischer, D. (2016). Wirtschaftsspionage. Phänomenologie – Erklärungsansätze - Handlungsoptionen. Wiesbaden: Springer Vieweg

Flores, W. R., Holm, H., Nohlberg, M. & Ekstedt., M. (2014). Investigating personal characteristics of phishing and the effect of national culture, Information & Computer Security, 23(2), 178–199.

Gupta, B. B., Tewari, A., Jain, A. K. & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629–3654.

Hadnagy, C. (2011). Die Kunst des Human Hacking. Heidelberg, München, Landsberg, Frechen, Hamburg: mitp.

Hadnagy, C. (2014). Social Engineering enttarnt: [Sicherheitsrisiko Mensch]. Frechen: mitp Verlag.

Halevi, T., Memon, N. & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks. SSRN Electronic Journal. 10.2139/ssrn.2544742.

Happy, H. (2016). NEO-PI-R. NEO-Persönlichkeitsinventar nach Costa und McCrae. Göttingen: Hogrefe Verlag.

Hofstede, G. (1980). Culture's consequences. International differences in work-related values. Beverly Hills: Sage.

Janneck, M. (2007). Quadratische Kommunikation im Netz: Gruppeninteraktion und die Gestaltung von CSCL-Systemen. Lohmar: Eul.

Lipski, M. (2009). Social Engineering. Der Mensch als Sicherheitsrisiko in der IT. Hamburg: Diplomica.

Long, J., Pinzon, S., Wiles, J. & Mitnick, K. D. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington: Syngress.

Maro, F. (2012). Von netten und anderen Menschen. Berlin: epubli.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and Information Security Awareness, Computers in Human Behaviour, 69, 151–156.

Mitnick, K. D. & Simon, W. L. (2006). Die Kunst der Täuschung. Risikofaktor Mensch. Mitp-Verlag.

Montada, L. & Lerner, M. J. (1998). Responses to victimizations and belief in a just world. New York: Plenum Press.

Neely, L. (2017). 2017 Threat Landscape Survey: Users on the Front Line. Verfügbar unter: https://www.sans.org/reading-room/whitepapers/analyst [20.07.2018]

Pohlmann, R. & Linnemann, M. (2010). Sicher im Internet - Tipps und Tricks für das digitale Leben. Zürich: Orell Füssli.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D. & Jerram, C., (2015). Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? In F. Burstein et al (Eds.) Proceedings of Australian Conference of Information Systems.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Computers & Security, 66, 40–51.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2013). Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In L. J. Janczewski et al. (Eds.), Security and Privacy Protection in Information Processing Systems-IFIP Advances in Information and Communication Technology, Springer, Berlin.

Pattinson, M., Butavicius, M, Parsons, K., McCormac, A. & Calic, D. (2015). Factors that influence Information Security Behaviour: An Australian web-based study". In T. Tryfonas & I. Askoxylakis (Eds.), Proceedings of Third International Conference on Human Aspects of Information Security, Privacy and Trust (HAS 2015), Los Angeles, USA.

Pattinson, M., Jerram, C., Parsons, K. M., McCormac, A. & Butavicius, M. A. (2012). Why do some people manage phishing emails better than others? Information Management & Computer Security, 20(1), 18–28.

Rammstedt, B. Christoph J. Kemper, C. J., Klein, M. C., Beierlein, C. & Kovaleva, A. (2012). Eine kurze Skala zur Messung der fünf Dimensionen der Persönlichkeit. Big-Five-Inventory-10 (BFI-10). Mannheim: GESIS (Working papers / GESIS, 23).

Röttgerkamp, A. (2018). Wie infiziert sind wir? Malware – Die unsichtbare Bedrohung. Netzsieger. Verfügbar unter: https://www.netzsieger.de/ratgeber/malware-statistiken [20.05.2018]

Schaumann, P. (2017). Schutz gegen Social Engineering – neue psychologische Ansätze. Verfügbar unter: http://sicherheitskultur.at/social_engineering.htm [17.05.2018]

Schein, Edgar H. (1985). Organizational culture and leadership: a dynamic view. San Francisco: Jossey-Bass.

Schmidt, P., Bamberg,S., Davidov, E., Herrmann, J. & Schwartz, S. H. (2007). Die Messung von Werten mit dem «Portraits Value Questionnaire». Zeitschrift für Sozialpsychologie 38(4), S. 261–275.

Schumacher, S. (2013). Die psychologischen Grundlagen des Social-Engineerings. Wittenberg: DGI-Forum.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010), "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In E. Mynatt et al. (Eds.) Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '10), Atlanta, GA, USA.

Steinmetz, H., Schmidt, P., Tina-Booh, A., Wieczorek, S., & Schwartz, S. H. (2009). Testing measurement invariance using multigroup CFA: Differences between eductional groups in human values measurement. Quality and Quantity, 43, 599–616.

Stöcker, C. (2011). Nerd Attack! Eine Geschichte der digitalen Welt vom C64 bis zu Twitter und Facebook. DVA Sachbuch.

Schwartz, S. H. (1994). Are there universal aspects in the content and structure of values? Journal of Social Issues, 50, 19–45.

Staar, H., Keysers, P., Storch, F., Kempny, Ch. & Janneck, M. (2015). Political Skills 2.0 - An Analysis of Success-oriented Strategic Behavior in Online Business Networks. In Proceedings of WEBIST 2015 - 11th International Conference on Web Information Systems and Technologies. SciTePress (pp. 670–671).

Tembe, R., Zielinska, O., Liu, Y., Wha Hong, K., Murphy-Hill, E., Mayhorn, C. and Ge, S. (2014). Phishing in International Waters: Exploring Cross-National Differences in Phishing Conceptualizations between Chinese, Indian and American Samples. In L. A. Williams et al. (Eds.) Proceedings of the 2014 Symposium and Bootcamp on the Science of Security (HotSoS '14), Raleigh, NC, USA.

Uebelacker, S. & Quiel, S. (2104). The Social Engineering Personality Framework. In G. Bella & G. Lenzini (Eds.), Proceedings of the 4th International Worskhop on Socio-Technical Aspects in Security and Fraud, NJ, USA, IEEE.

Vishwanath, Arun & Herath, Tejaswini & Chen, Rui & Wang, Jingguo & Raghav Rao, H. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems. 51. 576–586.

Watson, D., Holz, T. & Mueller, S. (2008). Know your Enemy: Phishing – Behind the Scenes of Phishing Attacks,16th August 2008.[Online]. Available: https://www.honeynet.org/papers/phishing